REMARKS

Applicants respectfully request favorable reconsideration of this application, as amended.

As a preliminary matter Applicants wish to thank the Examiner for the courtesies extended during the November 21, 2008 telephonic interview.

Claims 1-4 and 6-17 are pending. By this Amendment, Claims 1 and 6-8 have been amended to more clearly recite the subject matter intended to be claimed, as discussed in detail below. Claim 5 was previously cancelled without prejudice or disclaimer.

In the Office Action, the disclosure was objected to; Claims 6 and 15-17 were rejected under 35 U.S.C. § 101; and Claims 1-17 (although Claim 5 was previously cancelled) were rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Devine (U.S. 2005/0210296 A1, hereinafter "Devine") in view of Grantges (U.S. Patent No. 6,510,464, hereinafter "Grantges").

Objections to the Disclosure

In the Office Action, the disclosure was objected to for allegedly failing to disclose the apparatus claimed in Claims 6 and 15-17, and the media claimed in Claims 8-11. Applicants respectfully disagree.

Paragraphs [0013], [0014], and [0029] - [0033] of Applicants' disclosure, for example, clearly describe what the "apparatus" is (the system 1 is a computer system distributed and composed of machines 2a, 2b, 2c organized into one or more networks 3; the machines can be very diverse, such as for example, workstations, servers, routers, specialized machines, telephones or gateways between machines) and what the "apparatus" does (the security module includes analyzing means that make it

possible to request a certificate of the user from the client machine 2a, retrieve the

certificate requested from the client machine and send it to the server machine 2b in a

cookie header of HTTP requests).

Paragraphs [0032] – [0034] of Applicants' disclosure, for example, clearly

describe the method by which the certificate is transmitted between the client machine

and the server machine (via the security machine using a software module).

Additionally, paragraph [0055] clearly describes that a software program integrated

into the security module allows this method to be executed when the program is run.

Therefore, Applicants respectfully submit that the claimed "apparatus" and

"media" are clearly described in the specification.

Accordingly, Applicants respectfully request that the objection to the

disclosure be withdrawn.

Rejection Under 35 U.S.C. § 101

In the Office Action, Claims 6 and 15-17 were rejected under 35

U.S.C. § 101, for allegedly containing non-statutory subject matter. More

specifically, the Office Action alleges that the claimed apparatus is not

supported by the Specification as the machine described therein is directed

towards computer software and not to a physical device or piece of hardware.

Applicants respectfully disagree.

The term "security machine" as recited in Claims 6 and 15-17 is

described in detail in various portions of Applicant's disclosure as a physical

device or item of hardware. For example:

> "[0013] A shown in Fig.1, the system 1 is distributed and
> composed of machines 2a, 2b, 2c organized into one or more

networks 3. A machine 2 is very large conceptual unit that
includes both hardware and software...".

"[0029] In the system 1, the security module 2c handles a
security protocol. <u>The security module 2c is in the form of a
machine 2</u>...".

"[0030] In the embodiment of the invention illustrated in Fig.1,
the <u>security module 2c is an intermediate machine 2</u>. The
security module 2c, called a security front-end box, is split off
upstream from the server machine 2b".

See paragraphs [0013], [0029] and [0030] of Applicant's disclosure (underlines
added).

As the above-noted portions of Applicants' disclosure make clear, the security

machine is a piece of hardware or a physical device and not just computer software.

Therefore, Applicants respectfully submit that the claimed "apparatus"

comprising the "security machine" is directed to statutory subject matter.

Accordingly, Applicant respectfully requests that the rejection under § 101 be

withdrawn.

Rejection Under 35 U.S.C. § 103(a)

Turning to the rejections under 35 U.S.C. § 103(a), without acceding thereto,

independent Claim 1 has been amended to recite certain distinctive features of

Applicants' invention with greater particularity. For example, as now set forth in

Claim 1, the method of communicating to a server machine a certificate of a user

which is sent by a client machine via a security module comprises, *inter alia*,

<u>transmitting said certificate from the client machine to said security module using a</u>

<u>secure stateless protocol, inserting said certificate unmodified into a cookie header of</u>

<u>a request in a non-secure stateless protocol, the inserting being done by the security</u>

<u>module, and transmitting the request including the cookie header containing the</u>

unmodified certificate from the security module to the server machine using the non-secure protocol.

It is apparent that the applied references fail to teach or suggest at least these features. For example, Devine teaches a method and system for implementing a series of security protocols to protect remote user communications with remote enterprise services, the system including a client machine, a server machine and a security web server. However, Devine's method uses a secure version of the HTTP stateless protocol. *See* Devine, paragraph [0066]. Therefore, even assuming *arguendo* that the web server of Devine inserts a certificate into a cookie header unmodified and sends a request including the cookie header containing the unmodified certificate to the server machine, the request cannot be sent using a non-secure stateless protocol, as required in Claim 1, because only secure protocols are used in Devine.

Additionally, Devine discloses associating a given secure stateless protocol with a cookie. However, the cookie in Devine is generated by the server and is sent to the client machine. *See* Devine, paragraph [0066]. Therefore, even assuming *arguendo* that Devine discloses inserting an unmodified certificate into a cookie header, the cookie header is not transmitted from the security module to the server machine, as required in Claim 1, but from the server to the client machine.

Moreover, as acknowledged by the Office Action, Devine fails to disclose inserting a certificate unmodified into a cookie header. The Office Action, however, alleges that Grantges remedies Devine's deficiencies in this regard. Applicants respectfully disagree. Grantges appears to disclose sending a certificate from the client machine to a proxy 34 where a plug-in 36 associated with the proxy 34 extracts

the certificate from the message and passes it to a proxy server 40 in a header. The

certificate is authenticated by an authorization server 46 associated with the proxy

server 40, and the authentication data is returned to proxy server 40, which then

generates different cookies 90, 92 containing different information, which are later

sent to the client machine. Therefore, it is apparent that the certificate of Grantges is

inserted into a header when sent from plug-in 36 to proxy server 40, but it is not

inserted into a cookie header as required in Claim 1, because the cookie in Devine is

not generated by proxy 34 but by proxy server 40. Also, the cookie generated by

proxy server 40 does not include the unmodified certificate, as required in Claim 1.

At most, the cookie in Devine includes the authentication data generated by server 46

in response to the certificate being authorized. See Grantges, Col.9, lines 35-67, and

Col.10, lines 1-26.

Therefore, Applicants respectfully submit that Claim 1 distinguishes

patentably from Devine and Grantges, whether taken alone or in combination.

Claims 6, 7 and 8 also recite inserting the unmodified certificate into a cookie

header and transmitting a request including the cookie header containing the

unmodified certificate from the security machine (module) to a server machine using

a non-secure stateless protocol, and therefore, are also believed to distinguish

patentably from the applied references for at least the reasons as set forth above with

respect to Claim 1.

Claims 2-4, and 9-17 are also believed to be patentable based on their

dependence from Claims 1, and 6-8, respectively, as well as due to the additional

subject matter recited in Claims 2-4, and 9-17.

In view of the foregoing, Applicants respectfully submit that this application is in condition for allowance. Accordingly, a prompt Notice of Allowance is respectfully solicited.

The Commissioner is hereby authorized to charge to Deposit Account No. 50-1165 (T2147-907679) any fees under 37 C.F.R. §§ 1.16 and 1.17 that may be required by this paper and to credit any overpayment to that Account. If any extension of time is required in connection with the filing of this paper and has not been separately requested, such extension is hereby requested.

Respectfully submitted,

Date: December 4, 2008   By: _____
                                              Eric G. King
                                              Reg. No. 42,736

Miles & Stockbridge, P.C.   Otilia Gabor
1751 Pinnacle Drive   Reg. No. 60,217
Suite 500
McLean, Virginia 22102-3833
Telephone: (703) 610-8647